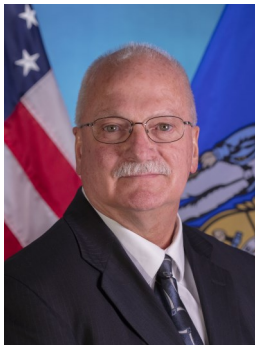
Josh Kaul
Attorney General

TIME System Newsletter

Volume 2020-1
February 2020

A Message From Our Director



I would like to introduce to you the TIME System Control Center (TSCC) staff that many of you talk to on a regular basis although you may not know them by name. Chris Kalina oversees TSCC as the TIME System Operations Manager. The TSCC staff includes the following broken down by currently assigned shifts. Midnights: Kent Christensen, Tina Harmon, and Jordan Lewis. Days: Patrick Gainey, Troy Hughes, and Dan Cook. Evenings: Bruce Bandt, Amber Hoefs, and Adelle Powers.

Wisconsin continues to make progress in our "Fix NICS" initiative to ensure all eligible warrants are entered in NCIC. With our programmatic changes and your ongoing efforts of reviewing your existing records, cancelling, and reentry when appropriate, as of February 1st, 2020, we had 88% of the felony warrants and 57% of the misdemeanor warrants in NCIC. Thank you for your assistance in ensuring all available warrants are visible to officers nationwide!

We continue to see an increase in volume of TIME System transactions. In 2019 the TIME System averaged 182,398 transactions per day. As of February 1st, the Wisconsin Hotfiles contained the following records: 132,714 Wanted Persons, 68,766 Prohibited Persons, 950 Missing Persons, 17,443 Protection Orders, 4820 Stolen/Felony Vehicles, 12,010 Stolen License Plates, 339 Stolen Parts, and 441,369 Concealed Carry Licenses (includes all license statuses).

We are anticipating the release of a Portal 100 service pack soon. In addition to updated code tables the service pack will offer some new Nlets functionality as described on page six (6) of this Newsletter.

Each agency with access to the TIME System is required to designate a Local Agency Security Officer (LASO). The FBI CJIS Division has implemented a new training requirement for each LASO that CIB will be releasing soon. For more information on this new training or a LASO in general please see page ten (10) of this Newsletter.

Remember it's time to complete your annual user validation. Please see page two (2) of this Newsletter if you are unfamiliar with this requirement or the process.

Please feel free to contact me or any of the CIB staff to discuss your thoughts on how we can continue to improve.

Walt Neverman

Walt Neverman
Director CIB

Inside this issue:

Annual User Validation	*2*
AMBER/Silver Alert Changes	*2*
CIB Only Warrants	*3*
LEOFA Form	*4*
Advanced Project Reminders	*5*
IP address changes	*5*
Return of Firearms	*6*
New Nlets Queries	*6*
Cyber Attacks Security Breaches	*7*
DOT Updates	*8*
2020 Audit Schedule	*9*
Hit Confirmation	*9*
LASO Training	*10*
CIB Contacts	*11*

Annual User Validation

The CJIS Security Policy section 5.5.1 Account Management requires that agencies validate their user accounts annually. Additionally, agencies are required to document when they conduct this validation process.

This simply means that at least once each year, agencies must review and validate their list of authorized users. This review should include TIME system users (eTIME, MDC, Portal 100, etc.) and users with physical and/or logical access to your secure location/network/systems (i.e. vendor, IT, cleaning personnel, etc.)

Once completed, this validation process needs to be documented in your agency records. This documentation may be needed as confirmation of user validation during your agency's TIME system audit.

This review should include removing access for those users no longer valid, ensuring the appropriate access levels are assigned to each user based on their duties and responsibilities, and ensuring the required background checks were completed, etc.

You should also ensure your agency's TRAIN roster only lists those who need TRAIN, TIME system, UCR or WIJIS access. If you have any questions, or need to make any changes please contact the Crime Information Bureau at cibtrain@doj.state.wi.us.

AMBER/Silver Alert Contact Information for DCI

Effective January 1, 2020: The first point of contact for requesting an AMBER Alert or a Silver Alert has changed. The new telephone number can be found on WILENET. After an alert has been approved, DCI will provide the agency with electronic submission forms. The new telephone number and additional information regarding the changes can be found on the secured side of WILENET (login is required prior to access of the below pages).

AMBER Alerts https://wilenet.org/secure/html/doj/amberalert/clearinghouse.html

Silver Alerts https://wilenet.org/secure/html/resources/newslinks/silver-alert.html

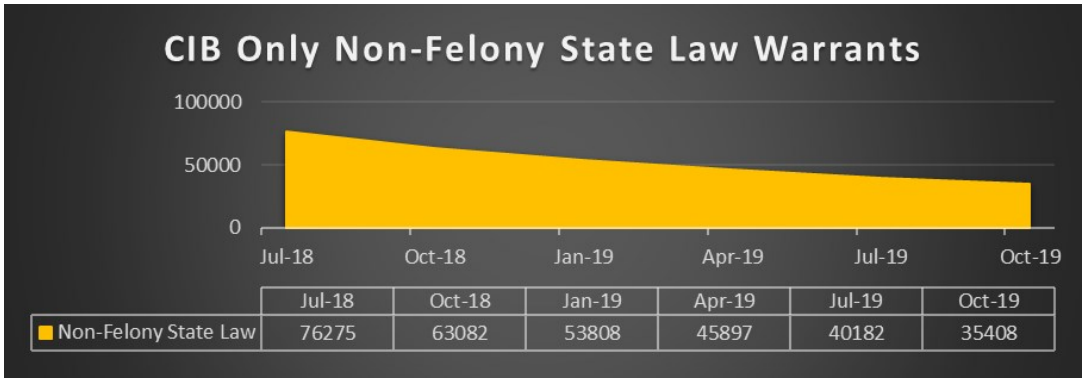
CIB Only Warrants

Since July 2018, CIB has been working with agencies to get **all** the CIB Only warrants that qualify to be entered into the NCIC Hotfile removed and added into **both** the NCIC & CIB Hotfiles.

At the beginning of this initiative there were over 83,000 felony and non-felony state law warrants entered into the CIB Only Hotfile. As of November 30, 2019, there are now 36,431 felony and non-felony state law warrants entered into the CIB Only Hotfile. A significant decrease, thank you!

Of the remaining 36,431, 2,046 of those are felony warrants and 34,385 are non-felony state law warrants. However, from an officer safety perspective **ALL** felony warrants and non-felony state law warrants should be entered into both the NCIC & CIB Hotfiles. The only exception would be if an individual already has more than one warrant entered for a specific agency.

	Jul-18	Oct-18	Jan-19	Apr-19	Jul-19	Oct-19
Felony	4064	3572	3291	2960	2714	2237



	Jul-18	Oct-18	Jan-19	Apr-19	Jul-19	Oct-19
Non-Felony State Law	76275	63082	53808	45897	40182	35408

One way to help your agency determine if there is a warrant that qualifies to be entered into both the NCIC & CIB Hotfiles is to review your agency warrants during monthly validation. If you come across a warrant that does not have a NCIC number associated with it, double check to see if it qualifies to be entered into the NCIC Hotfile. If yes, your agency should cancel and re-enter the warrant to ensure it's added to both the NCIC & CIB Hotfiles.

NCIC	Validation Exception	Record
		CIB

Law Enforcement Officer Flying Armed (LEOFA)

Did you know that there is a specific transaction that should be used when submitting a request to the Transportation Security Administration (TSA) for permission to fly armed? This transaction in Portal 100 can be found under Administrative Messages – O/S or Special Messages – (Form 0443 Law Enforcement Officer Flying Armed).

TSA requires the information within these requests be sent to them in a very specific format and requests will be denied if not submitted correctly. Proper use of this Portal form can prevent denials from TSA.

The most common errors are found in the name fields. Names must be submitted as Last Name, First Name in each unique Name field or the request to fly armed will be denied. Please see the screenshot below for an example.

Once you have received your approval with the unique alphanumeric identifier, be sure to print and bring a copy with you to the airport to provide to TSA. Remember to submit the form once for each direction of air travel.

Additional information regarding the LEOFA form can be found here

https://wilenet.org/html/cib/news-time/June2018timenews.pdf

Advanced Certification

TIME System Advanced certification is required for personnel who have successfully attained Basic TIME System certification and will perform entry, modify, supplemental and cancel transactions.

To obtain Advanced certification you can complete either classroom or online training. Advanced classroom instruction consists of a 2-day session. Advanced online training consists of 3 instructional modules:

1. Enter Person Records
2. Enter Vehicle Records (which includes license plates and parts)
3. Enter Other Property Records

The final score for Advanced TIME System certification is based on the grading of the 'Advanced Project' submitted by the student. The project materials will be received on the last day of classroom training or, for online training, download the project materials included in the Advanced Project module. Please keep these guidelines in mind when completing and submitting an Advanced Project!

- The project is due within 30 days of the last day of class or the starting date for the 'Advanced Project' module in TRAIN.
- Online students must complete the three entry modules before starting the 'Advanced Project' module in TRAIN; it will not count as completed unless they have been completed.
- Read all instructions carefully; points will be taken off if some steps are skipped!
- Keep all project-related printouts in chronological order.
- Make sure to include all relevant queries, as we can't give you credit without documentation. All data contained in an entry should be documented by the agency and can include the warrant itself, Criminal History Record (CHRI), DOT records, DOC records, etc.
- Another agency's warrants cannot be used as source documentation for your record entry. In a real-world scenario, you can reach out to the agency that issued the warrant and ask for any valid documentation they can share, such as Police Reports, Mug Shots, photos of tattoos, etc.

If you have any questions regarding your project, submit them to cibtrain@doj.state.wi.us. Provide your name, department and hours you are available in the event that a phone call is necessary. If you contact the Time System Control Center (TSCC) you will be referred to a CIB Training Officer.

IP Addresses

To prevent any service disruption, email CIBPSN@doj.state.wi.us before a Portal 100 workstation is moved or its IP address is changed.

Return of Firearms

In Wisconsin, a person may seek the return of property from the inventory of a law enforcement agency either through a process established by the agency or pursuant to a court order. In either instance, if the property is a firearm, the agency should conduct a firearms eligibility background check on the person to take possession of the firearm to determine if the person is eligible to receive that firearm. If the person is determined to be ineligible to receive the firearm under state or federal law, the agency may not transfer the firearm to that person. The state firearms eligibility laws are found in Wis. Stat. 941.29 and the federal firearms eligibility laws are found in 18 USC 922(g) and (n).

To assist agencies in conducting a firearms-level background check, the Crime Information Bureau of the Wisconsin Department of Justice has created a specialized transaction in the TIME System. Portal 100 form 0028 was created as a single form that will query all state and federal criminal justice databases needed to perform a complete firearms eligibility background check. Included in this transaction is a query of the FBI's National Instant Criminal Background Check System (NICS). Wisconsin's mental health prohibited records are included in the NICS Indices. It is important to note that because this transaction queries the NICS, this transaction may be used by law enforcement ONLY **for the return of a firearm and for no other purpose.**

It is the responsibility of the agency to apply the state and federal disqualifiers to the data returned in the queries. The state and federal disqualifiers are complicated, especially 18 USC 922(g)(9) – a misdemeanor crime of domestic violence; and 18 USC 922(g)(3) – illegal drug use. If, after the review of the information returned in the background check and the subsequent research of that information, the agency is unsure of the firearms eligibility status of the person, the agency may contact the Firearms Unit of CIB for assistance. Staff of the Firearms Unit will assist in the review of the information returned in the background check. Note that the Firearms Unit will not have the authority to query the NICS to assist the agency in its determination. Therefore, it is important that prior to contacting the Firearms Unit, the agency run transaction 0028 and review the information returned. The Firearms Unit may be contacted via email at wihotline@doj.state.wi.us.

New Nlets Queries - Coming Soon

State Statute codes - Transaction 0181 (Portal 100 form 0181) - Query a statue number and the destination state. The main purpose of this query is to allow the user to research the state statute code to identify the proper NCIC code. This query will be very useful when entering warrants.

VIN - Transaction 0405 (Portal 100 form 0405) - Query a VIN number. The query response will include characteristics on that particular VIN.

Hazmat - Transaction 1118 (Portal 100 form 1118) - Query a Hazardous Material by the chemical name.

All forms will be menu items located under NLETS/NCIC Special Messages

Houston, We've Got A Problem

What do you do when your agency experiences a cyber-attack and/or security breach?

If your agency experiences a security breach such as a virus or malware detected on a workstation, unusual activity on your network from a known/unknown botnet or your agency receives a ransomware attack, to name a few, do you have a security incident plan that outlines the steps you take to resolve the breach?

Whether or not the security incident directly or indirectly affects your agency, your first and second contact should always be to your agency Information Technology (IT) department and your local system administrator. Once you have your agency IT working on the incident, CJIS policy (section 3.2.9 and 5.3.1) requires that your agency notify CIB of the incident and status as soon as possible.

As the CJIS Systems Agency (CSA), CIB's responsibility is to make sure the security breach does not endanger the security or integrity of criminal justice information. In that respect CIB will work directly with the agency and IT staff to help resolve the problem and/or provide resources. Depending on the scope of the breach it may be determined that CIB would need to temporarily disconnect your agency's TIME System access while we work with your agency to create new user credentials (i.e. new userids and passwords) for those applications that access the TIME System (i.e. Portal 100, eTIME and S2S). The TIME and Tech Unit within CIB will work with your agency/TAC to update the credentials which will allow us to restore your agency's TIME System access as soon as possible. CIB would also require that your agency create new userids and password for proprietary applications that your agency uses to accesses the TIME System (i.e. Spillman, TriTech, New World, etc.).

Early detection and early notification can help to control the spread and damage of malicious cyber-attacks.

CIB – TIME System Control Center (TSCC)
Email: cibtscc@doj.state.wi.us or call (608) 266-7633

DCI – Wisconsin Statewide Intelligence Center (WISC):
Email: wisc@doj.state.wi.us or call (888) 324-9742 or (608-) 242-5393

Department of Transportation Updates

As of July 10th, 2019, paper temporary license plates issued by the Wisconsin Department of Transportation now contains a model description (Ex: Forester). This will replace the previously used model codes (Ex: 3644).

Paper temporary plates are to be placed in the lower corner of the rear window on the driver's side.

As of December 4, 2019, DOT no longer returns expired restrictions on a Wisconsin Driver Inquiry. This will prevent unnecessary review of restrictions that are no longer valid. The restrictions may still appear on the physical operator's license; however, once the restrictions are no longer valid, DOT removes them from the TIME System response.

Example of previous response:

```
Probationary License Status=VAL Classes=D-VAL Expires=04/03/2020
    Restrictions=No Operation With Alcohol Level More Than .02 From
    01-25-2017 Through 11-24-2018; IID Reqd For CLS D Operation:
    Functioning IID Required From 01-25-2017 Through 11-24-2018; Corr
    Lenses
```

Example of current response:

```
Probationary License Status=VAL Classes=D-VAL Expires=04/03/2020
    Restrictions=Corr Lenses
```

2020
TIME System Audits

In 2017, CIB began a new approach to auditing agencies around the state. Previous practice involved a bit of randomized selection throughout each three-year audit cycle. As of 2017, CIB has been conducting audits using a more geographic approach. 2020 will be the final year of the current audit cycle (2018 – 2020) which means the northern third of the state will be scheduled for their audit in 2020.

Agencies within the following counties will be contacted this year with details regarding their TIME System audit: Ashland, Barron, Bayfield, Burnett, Chippewa, Door, Douglas, Florence, Forest, Iron, Langlade, Lincoln, Marathon, Marinette, Menominee, Oconto, Oneida, Polk, Price, Rusk, Sawyer, St. Croix, Taylor, Vilas, and Washburn. Additionally, District Attorney's offices across the state, who access the TIME System, will be scheduled for an audit in 2020 as well.

If you have any questions on the upcoming audits, please contact us at cibaudit@doj.state.wi.us. We'll be happy to answer any questions you may have.

Hit Confirmation

Imagine you're a patrol officer and you know a subject in your district frequently has warrants for his/her arrest. You know you will be in the vicinity of his/her residence during your patrol so you query the subject's name at the beginning of your shift and find out he/she has a warrant. You want to make sure it is valid so you ask Dispatch to send a Hit Confirmation request to verify it is still valid before you get there. Is this the correct process?

Hit Confirmation requests can only be sent once the subject **is within the immediate vicinity of the officer and the officer is capable of detaining the subject.** Hit Confirmation is the process by which an agency contacts the entering agency to verify that a record is still valid. The entering agency is required to respond advising that the warrant is still valid or not valid within specific time frames.

The one exception to this rule is when the Firearms Unit or National Instant Criminal background check System (NICS) sends a Hit Confirmation request. The Firearms Unit and NICS conduct background checks for firearm purchases and when issuing a concealed carry permit. They will not have the subject in custody, but a determination whether a warrant is valid is still required.

In the above scenario, phone contact or administrative messages can be made to inquire upon the status of a warrant prior to contact with a subject. However, hit confirmation will still need to be made once contact has been made with the subject before service of the warrant.

Local Agency Security Officer (LASO) Training

In 2019, the FBI updated the CJIS Security Policy (Version 5.8) to include new training requirements for Local Agency Security Officers (LASO).

Each agency with access to the TIME System is required to designate a LASO whose primary roles include the following:

1. Identify who is using the TIME System approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to these items.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure CIB is promptly informed of security incidents.

Beginning in 2020, CIB will provide the required annual LASO training as an online module in TRAIN. TACs and TRAIN Administrators will be able to assign this training and track its completion just as they would any other TIME System training. This training will include the following items:

1. The LASO's roles and responsibilities listed above.
2. Any additional LASO roles and responsibilities.
3. Summaries of state and national audit findings.
4. A review of the most recent changes to the CJIS Security Policy.

If you have any questions on this new training opportunity, please contact us at cibtrain@doj.state.wi.us.

CIB Contacts

	Name	Telephone	Fax Number	Email
Director	Walt Neverman	608-264-6207	608-267-1338	nevermanwm@doj.state.wi.us
Deputy Director	Bradley Rollo	608-261-8134	608-267-1338	rollobr@doj.state.wi.us
TIME & Technical Services Manager	Katie Schuh	608-266-0335	608-267-1338	schuhkr@doj.state.wi.us
Training Officer - Senior	Emily Freshcorn	608-261-5800	608-267-1338	freshcornek@doj.state.wi.us
Training Officer	Gregory Kosharek	608-261-7667	608-267-1338	kosharekgr@doj.state.wi.us
Training Officer	Sara Phelan	608-266-9341	608-267-1338	phelansm@doj.state.wi.us
TIME System Operations Manager	Chris Kalina	608-266-7394	608-267-1338	kalinaca@doj.state.wi.us
TIME Analyst	Sarah Steindorf	608-261-8135	608-267-1338	steindorfsr@doj.state.wi.us
TIME Analyst	Craig Thering	608-266-7792	608-267-1338	theringcd@doj.state.wi.us
TIME Analyst	Zach Polachek	608-264-9470	608-266-6924	polachekzd@doj.state.wi.us
TIME Analyst	Jeanette Devereaux-Weber	608-266-2426	608-267-1338	devereauxweberjd@doj.state.wi.us
TIME System Audits			608-267-1338	cibaudit@doj.state.wi.us
TIME Billing			608-267-1338	timebilling@doj.state.wi.us
AFIS Operations Manager	Adrianna Bast	414-382-7500	414-382-7507	bastar@doj.state.wi.us
Criminal History Section	Jon Morrison	608-261-6267	608-267-4558	morrisonjd@doj.state.wi.us
	Brandon Smith	608-266-0872	608-267-4558	smithbp@doj.state.wi.us
Firearms Unit	Andrew Nowlan	608-267-2776	608-267-1338	nowlanam@doj.state.wi.us
TRAIN		608-266-7792	608-267-1338	cibtrain@doj.state.wi.us
WIJIS Justice Gateway	Zach Polachek	608-264-9470	608-266-6924	wijis@doj.state.wi.us
TSCC		608-266-7633	608-266-6924	
WILENET		608-266-8800		wilenet@doj.state.wi.us

Check the WILENET website for additional data at www.wilenet.org